



D-1171

In re Application of	)	
Donald McCoy, et al.	)	
	)	
Serial No.: 10/620,911	)	Art Unit 3694
	)	
Confirmation: 8962	)	
	)	
Filed: July 15, 2003	)	Patent Examiner
	)	Hai Tran
	)	
Title: AUTOMATED BANKING	)	
MACHINE BOOTABLE	)	
MEDIA AUTHENTICATION	)	

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

**BRIEF OF APPELLANTS PURSUANT TO 37 C.F.R. § 41.37**

Sir:

The Appellants hereby submit their Appeal Brief pursuant to 37 C.F.R. § 41.37 concerning the above-referenced Application.

06/23/2010 S/EWD/IE1 00000010 090428 10620911  
01 FC:1402 540.00 DA

**(i)**

**REAL PARTY IN INTEREST**

The Assignee of all right, title and interest to the above-referenced Application is Diebold Self-Service Systems division of Diebold Incorporated, an Ohio corporation.

**(ii)**

**RELATED APPEALS AND INTERFERENCES**

Appellants, Appellants' legal representative, and the Assignee of the present application are not aware of any prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or have a bearing on the Board's decision in the pending appeal.

**(iii)**

## **STATUS OF CLAIMS**

Claims 1-34 are pending in the Application.

Claims rejected: 1-34

Claims allowed: none

Claims confirmed: none

Claims withdrawn: none

Claims objected to: none

Claims canceled: none

Appellants appeal the rejections of claims 1-34. These claim rejections were the only claim rejections present in the final Office Action (“Action”) dated January 27, 2010. Claims 1-34 have been at least twice rejected.

**(iv)**

**STATUS OF AMENDMENTS**

A final rejection was made January 27, 2010. No amendments to the claims were requested to be admitted after the non-final rejection.

(v) **SUMMARY OF CLAIMED SUBJECT MATTER**

*Concise explanations of exemplary forms of the claimed invention:*

**With Respect to Independent Claim 1**

Claim 1 defines subject matter that is directed to a method of operating an automated banking machine (10) (Figures 1 and 2; Page 8, lines 7-8). As discussed at page 14, lines 1-7, the method includes a step (a) in which a computer (30) (Figure 2) in the automated banking machine, detects the presence of bootable media (e.g., floppy disk, CD, DVD, USB media) in at least one alternative storage device drive, such as a floppy disk drive (62), CD-ROM drive (64), DVD Drive (66), USB port (70) of the automated banking machine (Page 10, lines 4-15).

As discussed at Page 13, lines 1-21 and illustrated in Figures 4 and 5, the computer (10) includes a BIOS (50, 100) that specifies which of a plurality of storage device drives corresponds to a default storage device drive (114, 120) (e.g., a hard drive) which does not require an input of a first BIOS password (110, 116), and which of the plurality of storage device drives corresponds to the at least one alternative storage device drive (106, 108, 118) such as floppy disk drive (104) and CD-ROM drive (106) which does require the input of the BIOS boot password (110, 116).

In this described example, the method also includes a step (b) (discussed at page 15, lines 2-6) of booting the computer responsive to a boot record on either the bootable media of the at least one alternative storage device drive or a bootable media of the default storage device drive.

As discussed at page 14, line 8 to page 15, line 4, when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password. When the inputted password corresponds to

the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot record on the bootable media of the at least one alternative storage device drive.

As discussed at page 15, lines 4-7, when the bootable media of the at least one alternative storage device drive is not detected in step (a), the computer is booted responsive to a boot record on the bootable media of the default storage device drive without requiring a user to input the BIOS boot password.

#### **With Respect to Independent Claim 14**

Claim 14 defines subject matter that is directed to at least one article bearing computer executable instructions (50) (e.g., a BIOS) operative to cause a computer (30) in an automated banking machine (10) to cause the automated banking machine to carry out a method (Figure 2; Page 10, line 20 to page 11, line 5).

In an example embodiment, as discussed at page 14, lines 1-7, the method includes a step (a) in which a computer (30) (Figure 2) in the automated banking machine, detects the presence of bootable media (e.g., floppy disk, CD, DVD, USB media) in at least one alternative storage device drive, such as a floppy disk drive (62), CD-ROM drive (64), DVD Drive (66), USB port (70) of the automated banking machine (Page 10, lines 4-15).

As discussed at Page 13, lines 1-21 and illustrated in Figures 4 and 5, the computer (10) includes a BIOS (50, 100) that specifies which of a plurality of storage device drives corresponds to a default storage device drive (114, 120) (e.g., a hard drive) which does not require an input of a first BIOS password (110, 116), and which of the plurality of storage device drives corresponds to

the at least one alternative storage device drive (106, 108, 118) such as floppy disk drive (104) and CD-ROM drive (106) which does require the input of the BIOS boot password (110, 116).

In this described example, the method also includes a step (b) (discussed at page 15, lines 2-6) of booting the computer responsive to a boot record on either the bootable media of the at least one alternative storage device drive or a bootable media of the default storage device drive.

As discussed at page 14, line 8 to page 15, line 4, when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password. When the inputted password corresponds to the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot record on the bootable media of the at least one alternative storage device drive.

As discussed at page 15, lines 4-7, when the bootable media of the at least one alternative storage device drive is not detected in step (a), the computer is booted responsive to a boot record on the bootable media of the default storage device drive without requiring a user to input the BIOS boot password.

### **With Respect to Independent Claim 16**

Claim 16 defines subject matter that is directed to a method of operating an automated banking machine (10) (Figures 1 and 2; Page 8, lines 7-8). As discussed at page 14, lines 1-7, the method includes a step (a) in which a computer (30) (Figure 2) in the automated banking machine detects the presence of a first bootable media (e.g., disk media, floppy disk, CD, DVD, USB media) in at least one first storage device drive (44) of the automated banking machine (e.g., hard drive 60, floppy disk drive 62, CD-ROM drive 64, DVD Drive 66, USB port 70) (Page 10, lines 4-15).



In this described example, the method also includes a step (b) (discussed at page 15, lines 2-6) of booting the computer responsive to a boot record on either the first bootable media of the at least one first storage device drive or a second bootable media of a second storage device drive of the automated banking machine.

As discussed at page 13, line 1 to page 15, line 4 and illustrated in Figures 4 and 5, when the first bootable media is detected in step (a), the booting of the computer includes determining responsive to a BIOS (50, 100) of the automated banking machine that the at least one first storage device drive (106, 108, 118) such as floppy disk drive (104) or CD-ROM drive (106) requires a BIOS boot password (110, 116); and requiring at least once for a user to input the BIOS boot password. When an inputted password corresponds to a BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to a first boot record on the first bootable media.

As discussed at page 15, lines 4-7, when the first bootable media is not detected in step (a) the booting of the computer includes determining responsive to the BIOS of the automated banking machine that the second storage device drive (114, 120) (e.g., a hard drive) does not require the BIOS boot password (110, 116). The computer is then booted responsive to the boot record on the second bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

#### **With Respect to Independent Claim 17**

Claim 17 defines subject matter that is directed to at least one article bearing computer executable instructions (50) (e.g., a BIOS) operative to cause a computer (30) in an automated

banking machine (10) to cause the automated banking machine to carry out a method (Figure 2; Page 10, line 20 to page 11, line 5).

In an example embodiment, as discussed at page 14, lines 1-7, the method includes a step (a) in which a computer (30) (Figure 2) in the automated banking machine, detects the presence of a first bootable media (e.g., disk media, floppy disk, CD, DVD, USB media) in at least one first storage device drive (44) of the automated banking machine (e.g., hard drive 60, floppy disk drive 62, CD-ROM drive 64, DVD Drive 66, USB port 70) (Page 10, lines 4-15).

In this described example, the method also includes a step (b) (discussed at page 15, lines 2-6) of booting the computer responsive to a boot record on either the first bootable media of the at least one first storage device drive or a second bootable media of a second storage device drive of the automated banking machine.

As discussed at page 13, line 1 to page 15, line 4 and illustrated in Figures 4 and 5, when the first bootable media is detected in step (a), the booting of the computer includes determining responsive to a BIOS (50, 100) of the automated banking machine that the at least one first storage device drive (106, 108, 118) such as floppy disk drive (104) or CD-ROM drive (106) requires a BIOS boot password (110, 116); and requiring at least once for a user to input the BIOS boot password. When an inputted password corresponds to a BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to a first boot record on the first bootable media.

As discussed at page 15, lines 4-7, when the first bootable media is not detected in step (a) the booting of the computer includes determining responsive to the BIOS of the automated banking machine that the second storage device drive (114, 120) (e.g., a hard drive) does not require the BIOS boot password (110, 116). The computer is then booted responsive to the boot record on

the second bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

**With Respect to Independent Claim 19**

Claim 19 defines subject matter that is directed to a method of operating an automated banking machine (10) (Figures 1 and 2; Page 8, lines 7-8). As discussed at page 14, lines 1-7, the method includes a step (a) in which a computer (30) (Figure 2) of the automated banking machine detects that a bootable media (e.g., floppy disk, CD, DVD, USB media) is present in at least one alternative storage device drive such as a floppy disk drive (62), CD-ROM drive (64), DVD Drive (66), USB port (70) of the automated banking machine (Page 10, lines 4-15), wherein a BIOS of the computer specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive.

As discussed at Page 13, lines 1-21 and illustrated in Figures 4 and 5, the computer (10) includes a BIOS (50, 100) that specifies that a BIOS password (110, 116) is required for the bootable media of the at least one alternative storage device drive (106, 108, 118) such as floppy disk drive (104) and CD-ROM drive (106).

In addition, as discussed at page 14, lines 8-10, the method may include a step (b) of prompting at least once for a user to input the BIOS boot password. In addition, as discussed at page 14, lines 13-15, the method may include a step (c) of determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer. Also, as discussed at page 15, lines 2-4, the method may include a step (d) of booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive (Page 10, lines 8-12).

In addition, the method may include a step (e) of restarting (e.g., booting) the computer to carry out alternative steps as discussed at page 15, lines 5-7. Here the method may include a step (f) of detecting with the computer that a bootable media is not present in the at least one alternative storage device drive (Page 15, lines 4-5); and a step (g) of booting the computer responsive to a boot record on a bootable media of a default storage device drive (114, 120) (e.g., a hard drive) without requiring a user to input the BIOS boot password (110, 116) (page 15, lines 5-7).

#### **With Respect to Independent Claim 20**

Claim 20 defines subject matter that is directed to at least one article bearing computer executable instructions (50) (e.g., a BIOS) operative to cause a computer (30) in an automated banking machine (10) to cause the automated banking machine to carry out a method (Figure 2; Page 10, line 20 to page 11, line 5).

In an example embodiment, as discussed at page 14, lines 1-7, the method includes a step (a) in which a computer (30) (Figure 2) of the automated banking machine detects that a bootable media (e.g., floppy disk, CD, DVD, USB media) is present in at least one alternative storage device drive such as a floppy disk drive (62), CD-ROM drive (64), DVD Drive (66), USB port (70) of the automated banking machine (Page 10, lines 4-15). A BIOS of the computer specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive.

As discussed at Page 13, lines 1-21 and illustrated in Figures 4 and 5, the computer (10) includes a BIOS (50, 100) that specifies that a BIOS password (110, 116) is required for the bootable media of the at least one alternative storage device drive (106, 108, 118) such as a floppy disk drive (104) and CD-ROM drive (106).

In addition, as discussed at page 14, lines 8-10, the method may include a step (b) of prompting at least once for a user to input the BIOS boot password. In addition as discussed at page 14, lines 13-15, the method may include a step (c) of determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer. Also, as discussed at page 15, lines 2-4, the method may include a step (d) of booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive (Page 10, lines 8-12).

In addition, the method may include a step (e) of restarting (e.g., booting) the computer to carry out alternative steps as discussed at page 15, lines 5-7. Here the method may include a step (f) of detecting with the computer that a bootable media is not present in the at least one alternative storage device drive (Page 15, lines 4-5); and a step (g) of booting the computer responsive to a boot record on a bootable media of a default storage device drive (114, 120) (e.g., a hard drive) without requiring a user to input the BIOS boot password (110, 116) (page 15, lines 5-7).

#### **With Respect to Independent Claim 22**

Claim 22 defines subject matter that is directed to an automated banking machine (10) comprising a computer (30). (Figure 2; Page 9, lines 7-8). The computer includes a BIOS (50) (Page 10, lines 20-21) that includes a BIOS boot password (110) (Figure 4; Page 13, lines 13-15). In addition the BIOS specifies a default storage device drive (114) (e.g., a hard drive) which does not require a boot password.

As shown in Figures 1 and 2 and discussed at page 8, line 15 to page 9, line 10, the automated banking machine may include at least one input device (32) (e.g., keypad 16, function

keys 14, card reader 22) and at least one transaction function device (36) (e.g., cash dispenser 24, depository 26) in operative connection with the computer.

Also, as shown in Figures 2-5 and discussed at page 10, lines 4-15 and page 13, lines 13-21, the automated banking machine may include at least one first storage device drive (106, 108, 118) (e.g., floppy disk drive 104 and CD-ROM drive 106) and a second storage device drive (114, 120) (e.g., a hard drive) in operative connection with the computer. The second storage device drive corresponds to the default storage device drive specified in the BIOS.

As discussed at page 14, line 8 to page 15, line 4, when the computer detects a bootable media associated with the at least one first storage device drive, the computer is operative to require a user to input a BIOS boot password through the at least one input device prior to booting responsive to a boot record associated with the bootable media of the at least one first storage device drive.

Further, as discussed at page 15, lines 4-7, when the computer does not detect a bootable media associated with the at least one first storage device drive, the computer is operative to boot responsive to a boot record on a bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

**(vi) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

The grounds to be reviewed in this appeal are:

Whether Appellants' claims 1-34 are obvious under 35 U.S.C. § 103(a) over  
Cromer, et al., U.S. Publication No. 2002/0166072 ("Cromer").

(vii)

## ARGUMENT

### The 35 U.S.C. § 103 (a) Rejections

#### The Applicable Legal Standards

In order to present a valid rejection based on obviousness, it is first necessary for the Office to make a *prima facie* showing of obviousness. *Prima facie* obviousness requires a showing that each of the recited features and relationships in the claims was known in the prior art. If the Office fails to establish a *prima facie* case of obviousness, the Appellant is under no obligation to submit evidence of nonobviousness. MPEP § 2142.

Even in cases where the Office has made a *prima facie* showing of obviousness, a rejection cannot be properly made unless there is a requisite showing that it would be obvious to one having ordinary skill in the art to combine the features and relationships to produce the invention as claimed. In accordance with the dictates of the United States Supreme Court in *KSR Int'l. Co. v. Teleflex, Inc.*, 127 S.Ct. 1727, 82 USPQ 2d 1385 (2007) the determination as to whether there is a reason to combine features of prior art references must be evaluated through an analysis of the factors recited in *Graham v. John Deere*, 383 U.S.1, 148 USPQ 459 (1966). The factual inquiries that must be made under *Graham* include:

- (a) determining the scope and content of the prior art;
- (b) ascertaining the differences between the prior art and the claims in issue;
- (c) resolving the level of ordinary skill in the pertinent art;
- (d) evaluating evidence of secondary considerations.



It is respectfully submitted that the Action from which this appeal is taken does not meet these burdens.

### **Rejections Under 35 U.S.C. § 103(a) Over Cromer**

In the Action, claims 1-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Cromer. These rejections are respectfully traversed.

### **Cromer**

As illustrated in Figure 1 and discussed in paragraph [0018], Cromer is directed to a computer system (10). In paragraph [0010], Cromer holds out as a problem with the prior art, that “it is a trivial exercise for an unauthorized user to connect his own hard disk drive in lieu of the password protected hard disk drive.” Cromer’s solution to making computers more secure and to prevent any portable unknown drive from being used to boot a computer, is to require the computer system be configured to only boot from devices that internally include data (e.g., model and serial number) stored thereon (referred to as a password) that has been previously coupled to the BIOS of the computer (Figure 2, paragraphs [0026] and [0027]).

### **Claim 1 (Grouped with independent claim 14 and dependent claims 3 and 7-13)**

Claim 1 is an independent claim directed to a method involving an automated banking machine. Claim 14 is an independent claim directed to an article bearing computer executable instructions reciting method steps corresponding to the steps recited in respective claim 1.

Claims 1 and 14 recite a BIOS of an automated banking machine that specifies a drive that (when detected) requires the manual input by a user of a BIOS boot password prior to booting

from the drive. Also the BIOS of the automated banking machine specifies a drive that does not require the manual input by a user of a BIOS boot password prior to booting from the drive.

This arrangement enables the automated banking machine to boot from its default internal hard drive automatically without user intervention. However, when an authorized technician wishes to conduct maintenance on the machine, the technician may attach a bootable portable drive and/or bootable media, which will be booted only after the person inputs a password that matches a password stored in the BIOS. With this configuration, the automated banking machine is operative to be booted by any portable drive and/or media the technician may choose to use, as long as the technician can manually input the proper boot password stored in the BIOS.

Nowhere does Cromer disclose or suggest an automated banking machine or any other machine with such features and capabilities. Further, even with respect to a generic computer system such as a PC, Cromer does not disclose or suggest these features. Rather in Cromer, a computer boots to a detected drive by verifying (when configured to do so) that a hash of data stored on the drive (e.g., a model and serial number) matches corresponding data stored in a BIOS (paragraph [0027]). Cromer does not disclose or suggest (or have any apparent reason for) after detection of bootable media for a designated drive, requiring that a user manually input a BIOS boot password in order to boot from the drive.

Thus claims 1 and 14 recite subject matter not disclosed or suggested by Cromer. For example nowhere does Cromer disclose or suggest the following combination of features, relationships and steps recited in claims 1 and 14:

- **wherein a BIOS of the computer specifies which of a plurality of storage device drives corresponds to a default storage device drive which does not require an input of a first BIOS password, and which of the plurality of**

**storage device drives corresponds to the at least one alternative storage device drive which does require the input of the BIOS boot password**

- **wherein when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password, wherein when the inputted password corresponds to the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot record on the bootable media of the at least one alternative storage device drive**

The Action appears to allege that Figure 2A and paragraphs [0022] and [0026] of Cromer disclose requiring a user to input a password when an alternative storage device drive is detected. Appellants respectfully disagree.

Figure 2A and paragraph [0026] of Cromer show that Cromer may require a password for booting to a device. However, as shown in Figure 2A, item 128, and paragraph [0027], this password is not a user inputted password, but rather is acquired by the computer interrogating the device for the serial and model number stored thereon. Thus the password in item 128 of Figure 128 cannot correspond to the required user inputted BIOS boot password of claims 1 and 14.

In addition, Applicants respectfully submit that the “configuration password” discussed at paragraph [0022] also does not correspond to the recited required input of a BIOS boot password. Rather the “configuration password” is simply a password that is used to enter a BIOS configuration routine. As shown in Figure 2B of Cromer, the BIOS configuration routine is a program via which a user configures the boot priority for drives and whether a drive should be interrogated during the boot process for the previously described hash of data.

As discussed in paragraph [0022], the user is always presented with the ability to enter the BIOS configuration routine simply by pressing the function key (F1) at the appropriate time, regardless of whether drives are detected by the BIOS and regardless of whether a password is required to boot from a particular drive. Thus, the configuration password of Cromer also does not correspond to the BIOS boot password recited in claims 1 and 14.

In addition, it should be noted that claims 5 and 6 (which depend from claim 1) recite requiring a user to provide a second input of a password prior to running the BIOS setup program. At best, Cromer's configuration password for entering his BIOS configuration routine is analogous to the required **second input** in claims 5 and 6 for entering a BIOS setup program, and thus does not disclose or suggest anything analogous to the **input** in claim 1 that **is required to boot from the bootable media of the at least one alternative storage device drive**.

Appellants respectfully submit that nowhere does Cromer disclose or suggest requiring a user to input a BIOS boot password when a bootable media is detected in an alternative storage device, for a machine with a BIOS that specifies which of a plurality of storage device drives corresponds to a default storage device drive which does not require an input of a BIOS boot password.

Also the Action on page 3 appears to assert that paragraph [0024] of Cromer teaches using his/her own password in order to boot a device. Appellants respectfully disagree. Paragraph [0024] discloses that in a preferred embodiment, the unique device password for the boot device is a combination of the model and serial numbers of the boot device. Paragraph [0024] of Cromer does not disclose another form of password for booting from a device. Thus paragraph [0024] does not provide any evidence that one of ordinary skill in the art at the time of the invention

would find it predictable to dispense with Cromer's described hashes and to use the process recited in claims 1 and 14.

In addition, it would not be obvious to one of ordinary skill in the art to modify Cromer in a manner that would correspond to the recited subject matter. In paragraph [0010], Cromer holds out as a problem with the prior art, that "it is a trivial exercise for an unauthorized user to connect his own hard disk drive in lieu of the password protected hard disk drive." Cromer's solution to making computers more secure and to prevent any portable unknown drive from being used to boot a computer, is to require the computer to be configured to only boot from devices that internally include data (e.g., model and serial number) that has been previously coupled to the BIOS of the computer. By calling out the disadvantage of using unknown hard disk drives (e.g., in paragraphs [0010] and [0028]), Cromer teaches away from Applicants' invention (which enables a technician to boot from a new and unknown drive/media) by teaching a system that prevents an unknown device (not coupled to a BIOS) from being booted. Further modifying Cromer as suggested in the Action to replace its hash method of coupling a drive to the BIOS, would destroy the utility and advantages of Cromer's described invention.

An obviousness rejection cannot be based on a combination of features in references if making the combination would result in destroying the utility or advantage of the device shown in the prior art references. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1598-99 (Fed. Cir. 1988). It follows that it would not be predictable to one of ordinary skill in the art at the time of the invention to modify Cromer as suggested in the Action.

In addition, Cromer does not disclose or suggest modifying an automated banking machine to include its described BIOS. An automated banking machine includes ports, such as USB ports

inside a locked enclosure and/or a locked safe. Cromer does not provide any teaching or suggestion that such physical security is inadequate.

Further, paragraph [0007] of Cromer (referenced in the Action to support obviousness) describes the lack of security associated with an unattended conventional PC. However, automated banking machines are not conventional PCs. For example, even when automated banking machines are unattended, the physical security of ports inside a locked enclosure or chest makes them non-analogous to a vulnerable unattended PC. Thus Cromer does not provide any motivation to one of ordinary skill in the art at the time of the invention to modify an automated banking machine to use his described BIOS.

In addition, Applicants have submitted evidence in the form of a Declaration under 37 C.F.R. § 1.132 that further provides evidence against a finding of obviousness. The Declaration (a copy of which is attached in Appendix ix) provides evidence that one of ordinary skill in the art at the time of the invention would not consider the subject matter recited in claims 1 and 14 as being obvious in view of Cromer. Also, it is well settled that “weight ought to be given to a persuasively supported statement of one skilled in the art on what was not obvious to him.” *In re Lindell*, 385 F.2d 453, 155 USPQ 521 (CCPA 1967). Applicants respectfully submit that the Declaration provides such a statement in addition to establishing that one of ordinary skill in the art at the time of the invention would consider the applied art as being **inoperative and non-enabling** with respect to the subject matter of the claims in the present application. Thus, the Declaration provides factual evidence which disproves the pending rejections.

Cromer does not disclose or suggest each of the features, relationships, and steps recited in claims 1 and 14 and the Office has not established *prima facie* obviousness. Also, because there is no apparent reason in the prior art or any other rationale for combining and/or modifying features

of the applied art so as to produce Appellants' invention, it is respectfully submitted that the 35 U.S.C. § 103(a) rejections of claims 1, 14 should be reversed. It also follows that the rejections of claims 1-13 and 15 which depend from the independent claims 1 and 14 should be reversed as well.

**Claim 2 (Grouped with Claim 23)**

With respect to claims 2 and 23, nowhere does Cromer disclose or suggest that when a bootable media of an alternative storage device drive is detected and a BIOS boot password is not inputted within a predetermined amount of time by a user, the computer is booted responsive to the boot record of the bootable media of the default storage device drive.

The Office's reasoning for why this feature would be an obvious modification to Cromer is unclear. With respect to claim 2, the Action asserts that "every ATM will abort your action if a user does not enter the password within a predetermined amount of time." In this example, it appears the Examiner may be referring to the entry of a PIN. However, a PIN is not analogous to the hash described in Cromer which couples a BIOS to a particular drive. There is no apparent reason for one of ordinary skill in the art to replace Cromer's use of a hash to couple a drive to a BIOS, with a PIN that times out after a predetermined amount of time. Such an asserted modification would reduce the security advantages provided by Cromer's invention, by allowing a user to connect and boot from an unauthorized drive by providing a PIN. Obviousness cannot be supported if the alleged modification (as is here) would destroy the utility and advantages of the reference.

For at least these reasons, the rejections of claims 2 and 23 should be reversed.

**Claim 4 (Grouped with Claim 34)**

With respect to claims 4 and 34, nowhere does Cromer disclose or suggest **a cash dispenser or dispensing cash from a cash dispenser**. Further, automated banking machines having cash dispensers are not analogous to Cromer's described vulnerable unattended conventional PC. Cromer does not provide any teaching or suggestion that the physical security of an automated banking machine is inadequate, and thus does not provide any apparent reason to modify an automated banking machine that dispenses cash to include his described BIOS.

The Action has not established a case of *prima facie* obviousness with respect to claims 4 and 34. Further, the Action has not provided any apparent reason or rationale to modify the applied art to correspond to the subject matter recited in claims 4 and 34.

Reversal of the rejections of claims 4 and 34 is respectfully requested.

**Claim 6 (Grouped with Claims 5, 32 and 33)**

Based on the objection to claims 5 and 6 in the Action, it appears that the Examiner may not have appreciated the differences between the recited BIOS boot password and the BIOS program password recited in the claims. It should be noted that Claim 6 (and Claim 33) recites both manual input of the BIOS boot password (recited in claims 1 and 22 from which they depend) and a different "BIOS program password." Nowhere does Cromer disclose or suggest two different distinct manually inputted passwords (one for entering a BIOS setup program; and another for determining whether to boot from a detected bootable media).

Also with respect to claim 5 (and claim 32), nowhere does Cromer disclose or suggest a single manually inputted password (one that is used for both entering a BIOS setup program; and for determining whether to boot from a detected bootable media).



Rather as pointed out previously, Cromer only includes a user provided configuration password in order to enter a configuration routine. An input of Cromer's configuration password is not used to boot from a detected bootable media.

For at least these reasons, the rejections of claims 5, 6, and 32 should be reversed.

**Claim 16 (Grouped with independent claim 17 and dependent claim 18)**

Claim 16 is an independent claim directed to a method involving an automated banking machine. Claim 17 is an independent claim directed to articles bearing computer executable instructions reciting method steps corresponding to the steps recited in respective claim 16.

Nowhere does Cromer disclose or suggest the following combination of features, relationships and steps recited in claims 16 and 17:

- **wherein when the first bootable media is detected in step (a), the booting of the computer includes:**
  - determining responsive to a BIOS of the automated banking machine that the at least one first storage device drive requires a BIOS boot password;**
  - requiring at least once for a user to input the BIOS boot password, wherein when an inputted password corresponds to a BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to a first boot record on the first bootable media; and**
- **wherein when the first bootable media is not detected in step (a) the booting of the computer includes:**

**determining responsive to a BIOS of the automated banking machine that the second storage device drive does not require the BIOS boot password, wherein the computer is booted responsive to the boot record on the second bootable media of the second storage device drive without requiring a user to input the BIOS boot password.**

Claims 16 and 17 were rejected in the Action under the same rationale provided in the Action with respect to claim 1. As discussed previously with respect to claim 1, the Action appears to allege that Figure 2A and paragraphs [0022] and [0026] of Cromer disclose requiring a user to input a password when an alternative storage device drive is detected. Appellants respectfully disagree.

Figure 2A and paragraph [0026] of Cromer show that Cromer may require a password for booting to a device. However, as shown in Figure 2A, item 128, and paragraph [0027], this password is not a user inputted password, but rather is acquired by the computer interrogating the device for the serial and model number stored thereon. Thus the password in item 128 of Figure 128 cannot correspond to the required user inputted BIOS boot password of claims 16 or 17.

In addition, Applicants respectfully submit that the “configuration password” discussed at paragraph [0022] does not correspond to the recited required input of a BIOS boot password either. Rather the “configuration password” is simply a password that is used to enter a BIOS configuration routine. As shown in Figure 2B of Cromer, the BIOS configuration routine is a program via which a user configures the boot priority for drives and whether a drive should be interrogated during the boot process for the previously described hash of data.

As discussed in paragraph [0022], the user is always presented with the ability to enter the BIOS configuration routine simply by pressing the function key (F1) at the appropriate time,

regardless of whether drives are detected by the BIOS and regardless of whether a password is required to boot from a particular drive. Thus, the configuration password of Cromer also does not correspond to the BIOS boot password recited in claims 16 and 17.

The Action on page 3 appears to assert that paragraph [0024] of Cromer teaches using his/her own password in order to boot a device. Appellants respectfully disagree. Paragraph [0024] discloses that in a preferred embodiment, the unique device password for the boot device is a combination of the model and serial numbers of the boot device. Paragraph [0024] of Cromer does not disclose another form of password for booting from a device. Thus paragraph [0024] does not provide any evidence that one of ordinary skill in the art at the time of the invention would find it predictable to dispense with Cromer's described hashes and instead carry out a method including determining responsive to a BIOS of the automated banking machine that the at least one first storage device drive requires a BIOS boot password and requiring at least once for a user to input the BIOS boot password, and wherein when the first bootable media is not detected, the method determines responsive to the BIOS that the second storage device drive does not require the BIOS boot password.

In addition, it would not be obvious to one of ordinary skill in the art to modify Cromer in a manner that would correspond to the recited subject matter. In paragraph [0010], Cromer holds out as a problem with the prior art, that "it is a trivial exercise for an unauthorized user to connect his own hard disk drive in lieu of the password protected hard disk drive." Cromer's solution to making computers more secure and to prevent any portable unknown drive from being used to boot a computer, is to require the computer to be configured to only boot from devices that internally include data (e.g., model and serial number) that has been previously coupled to the BIOS of the computer. By calling out the disadvantage of using unknown hard disk drives (e.g., in

paragraphs [0010] and [0028]), Cromer teaches away from Applicants' invention (which enables a technician to boot from a new and unknown drive/media) by teaching a system that prevents an unknown device (not coupled to a BIOS) from being booted. Further modifying Cromer as suggested in the Action to replace its hash method of coupling a drive to the BIOS, would destroy the utility and advantages of Cromer's described invention.

An obviousness rejection cannot be based on a combination of features in references if making the combination would result in destroying the utility or advantage of the device shown in the prior art references. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1598-99 (Fed. Cir. 1988). It follows that it would not be predictable to one of ordinary skill in the art at the time of the invention to modify Cromer as suggested in the Action.

In addition, Cromer does not disclose or suggest modifying an automated banking machine to include its described BIOS. An automated banking machine includes ports, such as USB ports, inside a locked enclosure and/or a locked safe. Cromer does not provide any teaching or suggestion that such physical security is inadequate.

Further, paragraph [0007] of Cromer (referenced in the Action to support obviousness) describes the lack of security associated with an unattended conventional PC. However, automated banking machines are not conventional PCs. For example, even when automated banking machines are unattended, the physical security of ports inside a locked enclosure or chest makes them non-analogous to a vulnerable unattended PC. Thus Cromer does not provide any apparent reason to one of ordinary skill in the art at the time of the invention to modify an automated banking machine to use his described BIOS.

In addition, Applicants have submitted evidence in the form of a Declaration under 37 C.F.R. § 1.132 that further provides evidence against a finding of obviousness. The Declaration

(a copy of which is attached in Appendix ix) provides evidence that one of ordinary skill in the art at the time of the invention would not consider the subject matter recited in claims 16 and 17 as being obvious in view of Cromer.

Cromer does not disclose or suggest each of the features, relationships, and steps recited in claims 16 and 17 and the Office has not established *prima facie* obviousness. Also, because there is no apparent reason in the prior art or any other rationale for combining and/or modifying features of the applied art so as to produce Appellants' invention, it is respectfully submitted that the 35 U.S.C. § 103(a) rejections of claims 16 and 17 should be reversed. It also follows that the rejection of claim 18 which depends from claim 17 should be reversed as well.

**Claim 19 (Grouped with independent claim 20 and dependent claims 21)**

Claim 19 is an independent claim directed to a method involving an automated banking machine. Claim 20 is an independent claim directed to articles bearing computer executable instructions reciting method steps corresponding to the steps recited in respective claim 19.

Nowhere does Cromer disclose or suggest the following combination of features, relationships and steps recited in claims 19 and 20:

- **wherein a BIOS of the computer specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive;**
- **b) prompting at least once for a user to input the BIOS boot password;**
- **c) determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer;**
- **d) booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive;**

- **e) restarting the computer;**
- **f) detecting with the computer that a bootable media is not present in the at least one alternative storage device drive; and**
- **g) booting the computer responsive to a boot record on a bootable media of a default storage device drive without requiring a user to input the BIOS boot password.**

Claims 19 and 20 were rejected in the Action under the same rationale provided in the Action with respect to claim 1. As discussed previously with respect to claim 1, the Action appears to allege that Figure 2A and paragraphs [0022] and [0026] of Cromer discloses requiring a user to input a password when an alternative storage device drive is detected. Appellants respectfully disagree.

Figure 2A and paragraph [0026] of Cromer show that Cromer may require a password for booting to a device. However, as shown in Figure 2A, item 128, and paragraph [0027], this password is not a user inputted password, but rather is acquired by the computer interrogating the device for the serial and model number stored thereon. Thus the password in item 128 of Figure 128 cannot correspond to the required user inputted BIOS boot password of claims 19 and 20.

In addition, Applicants respectfully submit that the “configuration password” discussed at paragraph [0022] also does not correspond to the recited required input of a BIOS boot password. Rather the “configuration password” is simply a password that is used to enter a BIOS configuration routine. As shown in Figure 2B of Cromer, the BIOS configuration routine is a program via which a user configures the boot priority for drives and whether a drive should be interrogated during the boot process for the previously described hash of data.

As discussed in paragraph [0022], the user is always presented with the ability to enter the BIOS configuration routine simply by pressing the function key (F1) at the appropriate time, regardless of whether drives are detected by the BIOS and regardless of whether a password is required to boot from a particular drive. Thus, the configuration password of Cromer also does not correspond to the BIOS boot password recited in claims 19 and 20.

The Action on page 3 appears to assert that paragraph [0024] of Cromer teaches using his/her own password in order to boot a device. Appellants respectfully disagree. Paragraph [0024] discloses that in a preferred embodiment, the unique device password for the boot device is a combination of the model and serial numbers of the boot device. Paragraph [0024] of Cromer does not disclose another form of password for booting from a device. Thus paragraph [0024] does not provide any evidence that one of ordinary skill in the art at the time of the invention would find it predictable to dispense with Cromer's described hashes and instead carry out a method with a BIOS that specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive, and also provides booting responsive to a boot record on a bootable media of a default storage device drive without requiring a user to input the BIOS boot password.

In addition, Cromer itself provides evidence that it would not be obvious to one of ordinary skill in the art to modify Cromer in a manner that would correspond to the recited subject matter. In paragraph [0010], Cromer holds out as a problem with the prior art, that "it is a trivial exercise for an unauthorized user to connect his own hard disk drive in lieu of the password protected hard disk drive." Cromer's solution to making computers more secure and to prevent any portable unknown drive from being used to boot a computer, is to require the computer to be configured to only boot from devices that internally include data (e.g., model and serial number) that has been

**previously coupled** to the BIOS of the computer. By calling out the disadvantage of using unknown hard disk drives (e.g., in paragraphs [0010] and [0028]), Cromer teaches away from Applicants' invention (which enables a technician to boot from a new and unknown drive/media) by teaching a system that prevents an unknown device (not coupled to a BIOS) from being booted. Further modifying Cromer as suggested in the Action to replace its hash method of coupling a drive to the BIOS, would destroy the utility and advantages of Cromer's described invention.

An obviousness rejection cannot be based on a combination of features in references if making the combination would result in destroying the utility or advantage of the device shown in the prior art references. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1598-99 (Fed. Cir. 1988). It follows that it would not be predictable to one of ordinary skill in the art at the time of the invention to modify Cromer as suggested in the Action.

In addition, Cromer does not disclose or suggest modifying an automated banking machine to include its described BIOS. An automated banking machine includes ports, such as USB ports inside a locked enclosure and/or a locked safe. Cromer does not provide any teaching or suggestion that such physical security is inadequate.

Further, paragraph [0007] of Cromer (referenced in the Action to support obviousness) describes the lack of security associated with an unattended conventional PC. However, automated banking machines are not conventional PCs. For example, even when automated banking machines are unattended, the physical security of ports inside a locked enclosure or chest makes them non-analogous to a vulnerable unattended PC. Thus Cromer does not provide any apparent reason to one of ordinary skill in the art at the time of the invention to modify an automated banking machine to use his described BIOS.



In addition, Applicants have submitted evidence in the form of a Declaration under 37 C.F.R. § 1.132 that further provides evidence against a finding of obviousness. The Declaration (a copy of which is attached in Appendix ix) provides evidence that one of ordinary skill in the art at the time of the invention would not consider the subject matter recited in claims 19 and 20 as being obvious in view of Cromer.

Cromer does not disclose or suggest each of the features, relationships, and steps recited in claims 19 and 20 and the Office has not established *prima facie* obviousness. Also, because there is no apparent reason in the prior art or any other rationale for combining and/or modifying features of the applied art so as to produce Appellants' invention, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection of claims 19 and 20 should be reversed. It also follows that the rejection of claim 21 which depends from claim 20 should be reversed as well.

**Claim 22 (Grouped with dependent claims 24-31)**

Claim 22 is an independent claim directed to an automated banking machine. Nowhere does Cromer disclose or suggest an automated banking machine with the following combination of features and relationships recited in claim 22:

- **wherein the BIOS includes a BIOS boot password;**
- **wherein when the computer detects a bootable media associated with the at least one first storage device drive, the computer is operative to require a user to input a BIOS boot password through the at least one input device prior to booting responsive to a boot record associated with the bootable media of the at least one first storage device drive;**

- **wherein the BIOS specifies a default storage device drive which does not require a boot password; wherein the second storage device drive corresponds to the default storage device drive specified in the BIOS;**
- **wherein when the computer does not detect a bootable media associated with the at least one first storage device drive, the computer is operative to boot responsive to a boot record on a bootable media of the second storage device drive without requiring a user to input the BIOS boot password.**

Claim 20 was rejected in the Action under the same rationale provided in the Action with respect to claim 1. As discussed previously with respect to claim 1, the Action appears to allege that Figure 2A and paragraphs [0022] and [0026] of Cromer discloses requiring a user to input a password when an alternative storage device drive is detected. Appellants respectfully disagree.

Figure 2A and paragraph [0026] of Cromer show that Cromer may require a password for booting to a device. However, as shown in Figure 2A, item 128, and paragraph [0027], this password is not a user inputted password, but rather is acquired by the computer interrogating the device for the serial and model number stored thereon. Thus the password in item 128 of Figure 128 cannot correspond to the required user inputted BIOS boot password of claim 22.

In addition, Applicants respectfully submit that the “configuration password” discussed at paragraph [0022] does not correspond to the recited required input of a BIOS boot password either. Rather the “configuration password” is simply a password that is used to enter a BIOS configuration routine. As shown in Figure 2B of Cromer, the BIOS configuration routine is a program via which a user configures the boot priority for drives and whether a drive should be interrogated during the boot process for the previously described hash of data.

As discussed in paragraph [0022], the user is always presented with the ability to enter the BIOS configuration routine simply by pressing the function key (F1) at the appropriate time, regardless of whether drives are detected by the BIOS and regardless of whether a password is required to boot from a particular drive. Thus, the configuration password of Cromer also does not correspond to the BIOS boot password recited in claim 22.

The Action on page 3 appears to assert that paragraph [0024] of Cromer teaches using his/her own password in order to boot a device. Appellants respectfully disagree. Paragraph [0024] discloses that in a preferred embodiment, the unique device password for the boot device is a combination of the model and serial numbers of the boot device. Paragraph [0024] of Cromer does not disclose another form of password for booting from a device. Thus paragraph [0024] does not provide any evidence that one of ordinary skill in the art at the time of the invention would find it predictable to dispense with Cromer's described hashes and instead produce a BIOS that requires a user to input a BIOS boot password through the at least one input device prior to booting responsive to a boot record associated with a bootable media of at least one first storage device drive.

In addition, Cromer itself provides evidence that it would not be obvious to one of ordinary skill in the art to modify Cromer in a manner that would correspond to the recited subject matter. In paragraph [0010], Cromer holds out as a problem with the prior art, that "it is a trivial exercise for an unauthorized user to connect his own hard disk drive in lieu of the password protected hard disk drive." Cromer's solution to making computers more secure and to prevent any portable unknown drive from being used to boot a computer, is to require the computer to be configured to only boot from devices that internally include data (e.g., model and serial number) that has been **previously coupled** to the BIOS of the computer. By calling out the disadvantage of using

unknown hard disk drives (e.g., in paragraphs [0010] and [0028]), Cromer teaches away from Applicants' invention (which enables a technician to boot from a new and unknown drive/media) by teaching a system that prevents an unknown device (not coupled to a BIOS) from being booted. Further modifying Cromer as suggested in the Action to replace its hash method of coupling a drive to the BIOS, would destroy the utility and advantages of Cromer's described invention.

An obviousness rejection cannot be based on a combination of features in references if making the combination would result in destroying the utility or advantage of the device shown in the prior art references. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1598-99 (Fed. Cir. 1988). It follows that it would not be predictable to one of ordinary skill in the art at the time of the invention to modify Cromer as suggested in the Action.

In addition, Cromer does not disclose or suggest modifying an automated banking machine to include its described BIOS. An automated banking machine includes ports, such as USB ports inside a locked enclosure and/or a locked safe. Cromer does not provide any teaching or suggestion that such physical security is inadequate.

Further, paragraph [0007] of Cromer (referenced in the Action to support obviousness) describes the lack of security associated with an unattended conventional PC. However, automated banking machines are not conventional PCs. For example, even when automated banking machines are unattended, the physical security of ports inside a locked enclosure or chest makes them non-analogous to a vulnerable unattended PC. Thus Cromer does not provide any apparent reason to one of ordinary skill in the art at the time of the invention to modify an automated banking machine to use his described BIOS.

In addition, Applicants have submitted evidence in the form of a Declaration under 37 C.F.R. § 1.132 that further provides evidence against a finding of obviousness. The Declaration

(a copy of which is attached in Appendix ix) provides evidence that one of ordinary skill in the art at the time of the invention would not consider the subject matter recited in claim 22 as being obvious in view of Cromer.

Cromer does not disclose or suggest each of the features and relationships recited in claim 22 and the Office has not established *prima facie* obviousness. Also, because there is no apparent reason in the prior art or any other rationale for combining and/or modifying features of the applied art so as to produce Appellants' invention, it is respectfully submitted that the 35 U.S.C. § 103(a) rejections of claim 22 should be reversed. It also follows that the rejection of claim 23-34 which depend from claim 22 should be reversed as well.

## CONCLUSION

Each of Appellants' pending claims specifically recites elements, relationships, and steps that are neither disclosed nor suggested in any of the applied prior art. Furthermore, the applied prior art is devoid of any apparent reason for producing the recited invention. For these reasons it is respectfully submitted that all the pending claims are allowable.

Respectfully submitted,



Ralph E. Jocke  
WALKER & JOCKE  
231 South Broadway  
Medina, Ohio 44256  
(330) 721-0000

Reg. No. 31,029

(viii)



## CLAIMS APPENDIX

1. A method comprising:

- a) detecting with a computer of an automated banking machine for the presence of a bootable media in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies which of a plurality of storage device drives corresponds to a default storage device drive which does not require an input of a first BIOS password, and which of the plurality of storage device drives corresponds to the at least one alternative storage device drive which does require the input of the BIOS boot password;
- b) booting the computer responsive to a boot record on either the bootable media of the at least one alternative storage device drive or a bootable media of the default storage device drive;

wherein when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password, wherein when the inputted password corresponds to the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot

record on the bootable media of the at least one alternative storage device drive; and

wherein when the bootable media of the at least one alternative storage device drive is not detected in step (a), the computer is booted responsive to a boot record on the bootable media of the default storage device drive without requiring a user to input the BIOS boot password.

2. The method according to claim 1, wherein when the bootable media of the at least one alternative storage device drive is detected in step (a) and the BIOS boot password is not inputted within a predetermined amount of time, in step (b) the computer is booted responsive to the boot record of the bootable media of the default storage device drive.

3. The method according to claim 1, wherein when the bootable media of the at least one alternative storage device drive is detected in step (a) and at least once the inputted password does not correspond to the BIOS boot password stored in the BIOS of the computer, in step (b) the computer is booted responsive to the boot record of the bootable media of the default storage device drive.

4. The method according to claim 1, and further comprising:

- c) executing at least one terminal control software component in the computer which is stored on the bootable media of the default storage device drive; and



- d) dispensing cash from a cash dispenser responsive to at least one terminal control software component.

5. The method according to claim 1, and further comprising:

- c) receiving a first input that is representative of a request to run a BIOS setup program; and
- d) requiring a user to provide a second input that corresponds to the BIOS boot password stored in the BIOS prior to running the BIOS setup program.

6. The method according to claim 1, and further comprising:

- c) receiving a first input that is representative of a request to run a BIOS setup program; and
- d) requiring a user to provide a second input that corresponds to a BIOS program password stored in the BIOS prior to running the BIOS setup program.

7. The method according to claim 6, wherein in steps (b) and (c) both the BIOS boot password and the BIOS program password are stored in the BIOS of the computer.

8. The method according to claim 1, wherein in step (b) the default storage device drive and associated bootable media correspond to a hard drive.
9. The method according to claim 8, wherein in step (b) the bootable media of the at least one alternative storage device drive corresponds to a portable media.
10. The method according to claim 9, wherein in step (b) the portable media corresponds to a floppy disk.
11. The method according to claim 9, wherein in step (b) the portable media corresponds to a CD.
12. The method according to claim 9, wherein in step (b) the portable media corresponds to a DVD.
13. The method according to claim 9, wherein in step (b) the portable media corresponds to a portable hard drive.
14. At least one article bearing computer executable instructions operative to cause a computer in an automated banking machine to cause the automated banking machine to carry out a method comprising:

- a) detecting with the computer of the automated banking machine, the presence of a bootable media in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies which of a plurality of storage device drives corresponds to a default storage device drive that does not require an input of a first BIOS password, and which of the plurality of storage device drives corresponds to the at least one alternative storage device drive that does require the input of the BIOS boot password;
- b) booting the computer responsive to a boot record on either the bootable media of the at least one alternative storage device drive or a bootable media of the default storage device drive;

wherein when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password, wherein when the inputted password corresponds to the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot record on the bootable media of the at least one alternative storage device drive; and

wherein when the bootable media of the at least one alternative storage device drive is not detected in step (a), the computer is booted responsive to

a boot record on the bootable media of the default storage device drive  
without requiring a user to input the BIOS boot password.

15. The at least one article according to claim 14, wherein the instructions include a file that is  
operative to update a flash memory device of the computer of the automated banking machine.

16. A method comprising:

- a) detecting with a computer of an automated banking machine, the presence of a first  
bootable media in at least one first storage device drive of the automated banking  
machine;
- b) booting the computer responsive to a boot record on either the first bootable media  
of the at least one first storage device drive or a second bootable media of a second  
storage device drive of the automated banking machine;

wherein when the first bootable media is detected in step (a), the booting of  
the computer includes:

determining responsive to a BIOS of the automated banking  
machine that the at least one first storage device drive requires a  
BIOS boot password;

requiring at least once for a user to input the BIOS boot password,  
wherein when an inputted password corresponds to a BIOS boot  
password stored in the BIOS of the computer, the computer is  
booted responsive to a first boot record on the first bootable media;  
and

wherein when the first bootable media is not detected in step (a) the booting  
of the computer includes:

determining responsive to a BIOS of the automated banking  
machine that the second storage device drive does not require the  
BIOS boot password, wherein the computer is booted responsive to  
the boot record on the second bootable media of the second storage  
device drive without requiring a user to input the BIOS boot  
password.

17. At least one article bearing computer executable instructions operative to cause a computer in  
an automated banking machine to cause the automated banking machine to carry out a method  
comprising:

- a) detecting with the computer of the automated banking machine, the presence of a  
first bootable media in at least one first storage device drive of the automated  
banking machine;

- b) booting the computer responsive to a boot record on either the first bootable media of the at least one first storage device drive or a second bootable media of a second storage device drive of the automated banking machine;

wherein when the first bootable media is detected in step (a), the booting of the computer includes:

determining responsive to a BIOS of the automated banking machine that the at least one first storage device drive requires a BIOS boot password;

requiring at least once for a user to input the BIOS boot password, wherein when an inputted password corresponds to a BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to a first boot record on the first bootable media; and

wherein when the first bootable media is not detected in step (a) the booting of the computer includes:

determining responsive to a BIOS of the automated banking machine that the second storage device drive does not require the BIOS boot password, wherein the computer is booted responsive to

the boot record on the second bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

18. The at least one article according to claim 17, wherein the instructions include a file that is operative to update a flash memory device of the computer of the automated banking machine.

19. A method comprising:

- a) detecting with a computer of an automated banking machine that a bootable media is present in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive;
- b) prompting at least once for a user to input the BIOS boot password;
- c) determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer
- d) booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive;
- e) restarting the computer;

- f) detecting with the computer that a bootable media is not present in the at least one alternative storage device drive; and
- g) booting the computer responsive to a boot record on a bootable media of a default storage device drive without requiring a user to input the BIOS boot password.

20. At least one article bearing computer executable instructions operative to cause a computer in an automated banking machine to cause the automated banking machine to carry out a method comprising:

- a) detecting with the computer of an automated banking machine that a bootable media is present in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive;
- b) prompting at least once for a user to input the BIOS boot password;
- c) determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer;
- d) booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive;



- e) restarting the computer;
- f) detecting with the computer that a bootable media is not present in the at least one alternative storage device drive; and
- g) booting the computer responsive to a boot record on a bootable media of a default storage device drive without requiring a user to input the BIOS boot password.

21. The at least one article according to claim 20, wherein the instructions include a file that is operative to update a flash memory device of the computer of the automated banking machine.

22. An automated banking machine comprising:

a computer, wherein the computer includes a BIOS, wherein the BIOS includes a BIOS boot password, and wherein the BIOS specifies a default storage device drive which does not require a boot password;

at least one input device in operative connection with the computer;

at least one transaction function device in operative connection with the computer; and

at least one first storage device drive and a second storage device drive in operative connection with the computer, wherein the second storage device drive corresponds to the

default storage device drive specified in the BIOS, wherein when the computer detects a bootable media associated with the at least one first storage device drive, the computer is operative to require a user to input a BIOS boot password through the at least one input device prior to booting responsive to a boot record associated with the bootable media of the at least one first storage device drive, wherein when the computer does not detect a bootable media associated with the at least one first storage device drive, the computer is operative to boot responsive to a boot record on a bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

23. The machine according to claim 22, wherein when the bootable media of the at least one first storage device drive is detected by the computer and the BIOS boot password has not been inputted thorough the at least one input device within a predetermined amount of time, the computer is operative to automatically boot responsive to the boot record associated with the bootable media of the second storage device drive.

24. The machine according to claim 22, wherein when the bootable media of the at least one first storage device drive is detected by the computer and at least one password inputted through the at least one input device does not correspond to the BIOS boot password, the computer is operative to automatically boot responsive to the boot record associated with the bootable media of the second storage device drive.

25. The machine according to claim 22, wherein the second storage device drive and associated bootable media corresponds to a hard drive.

26. The machine according to claim 25, wherein the bootable media for the at least one first storage device drive includes a portable bootable media.
27. The machine according to claim 26, wherein the portable bootable media includes a floppy disk.
28. The machine according to claim 26, wherein the portable bootable media includes a CD.
29. The machine according to claim 26, wherein the portable bootable media includes a DVD.
30. The machine according to claim 26, wherein the portable bootable media includes a portable hard drive.
31. The machine according to claim 22, wherein the at least one first storage device drive corresponds to a first portable storage device drive and a second portable storage device drive, wherein the second storage device drive corresponds to a hard drive, wherein the BIOS includes a boot order, wherein the boot order specifies a sequence for storage device drives in which the computer is operative to attempt to boot from, wherein the boot order includes the sequence of: the first portable storage media device drive, the second portable storage media device drive and the hard drive.
32. The machine according to claim 22, wherein the computer includes a BIOS setup program, wherein the computer is operative to require that a user input through the at least one input device,

the BIOS boot password prior to being granted access to modify the BIOS through the BIOS setup program.

33. The machine according to claim 22, wherein the computer includes a BIOS setup program and a BIOS program password, wherein the computer is operative to require that a user input through the at least one input device, the BIOS program password prior being granted access to modify the BIOS with the BIOS setup program.

34. The machine according to claim 22, wherein the transaction function device includes a cash dispenser, wherein when the computer has booted responsive to the boot record of the bootable media of the second storage device drive, the computer is operative to cause the cash dispenser to dispense cash responsive to at least one further input through the at least one input device.

**(ix)**

**EVIDENCE APPENDIX**

Declaration filed Under 37 C.F.R. § 1.132. dated October 5, 2009.



D-1171 R

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	)	
<b>Donald McCoy, et al.</b>	)	
	)	
Serial No.: <b>10/620,911</b>	)	Art Unit 3694
	)	
Confirmation: <b>8962</b>	)	
	)	
Filed: <b>July 15, 2003</b>	)	Patent Examiner
	)	Hai Tran
	)	
Title: <b>AUTOMATED BANKING</b>	)	
<b>MACHINE BOOTABLE</b>	)	
<b>MEDIA AUTHENTICATION</b>	)	

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**DECLARATION PURSUANT TO 37 C.F.R. § 1.132**

Sir:

I, Patrick C. Green, hereby declare as follows:

1. I am a former employee of Diebold, Incorporated and/or InterBold, a wholly owned subsidiary of Diebold, Incorporated (collectively referred to hereafter as "Diebold"). I was employed by Diebold as an engineer and engineering manager in the development of automated banking machines such as automated teller machines (ATMs)

and associated computer software for those machines. I retired from Diebold in 2007. I began working in the automated banking machine industry in approximately 1974.

2. Based on my knowledge and experience, a person having ordinary skill in the art of automated banking machines at time the present invention was made would have a four-year college degree in engineering, such as mechanical or electrical engineering, and have at least four years of experience in designing automated banking machines (or equivalent years of working experience in the design of automated banking machines).

3. I have reviewed the following references cited in the above-mentioned application (“application”):

- Cromer, et al., U.S. Publication No. 2002/0166072 (“Cromer”).

4. I have reviewed the subject matter disclosed in the application.

5. I have reviewed the claimed subject matter as set forth in the amendment filed in the Response dated August 12, 2009. A copy of the reviewed claims is attached.

6. There are significant differences between what is disclosed in the applied art of Cromer and what is claimed. For example, with respect to claims 1, 14, 16-17, 19-20, and 22, nowhere does the Cromer teach or suggest a BIOS of a computer of an automated banking machine (or any other machine) that specifies which of a plurality of storage device drives corresponds to a default storage device drive that does not require an input of a first BIOS password, and which of the plurality of storage device drives corresponds

to the at least one alternative storage device drive that does require the input of the BIOS boot password, such that: when the bootable media of the at least one alternative storage device drive is detected, the booting of the computer includes requiring at least once for a user to input a password . . .; and when the bootable media of the at least one alternative storage device drive is not detected, the computer is booted responsive to a boot record on the bootable media of the default storage device drive without requiring a user to input the BIOS boot password.

7. The recited subject matter (noted in paragraph 6) that is not disclosed or suggested in Cromer, would also not be considered obvious in view of Cromer by a person having ordinary skill in the art at the time of the invention.

For example, each of these claims recites a BIOS of an automated banking machine that specifies a drive that (when detected) requires the manual input by a user of a BIOS boot password prior to booting from the drive. Also the BIOS of the automated banking machine specifies a drive that does not require the manual input by a user of a BIOS boot password prior to booting from the drive.

This arrangement enables the automated machine to boot from its default internal hard drive automatically without user intervention. However, when an authorized technician wishes to conduct maintenance on the machine, the technician may attach a bootable portable drive/media, which will be booted only after the person inputs a password that matches a password stored in the BIOS. With this configuration, the automated banking machine is operative to be booted by any portable drive and/or media the technician may chooses to use, as long as the technician can manually input the



proper boot password stored in the BIOS.

Nowhere does Cromer disclose or suggest an automated banking machine or any other machine with such features and capabilities. Further, even with respect to generic PCs, Cromer does not disclose or suggest these features. For example, although Cromer shows (in Figure 2 and paragraph [0026]) that a password may be required to boot a device, as shown in Figure 2, item 128, and paragraph [0027], this password is not a user inputted password, but rather is acquired by the computer interrogating the device for the serial and model number stored thereon. In Cromer, a computer boots to a detected drive by verifying (when configured to do so) that a hash of data stored on the drive (e.g. a model and serial number) matches corresponding data stored in a BIOS (paragraph [0027]). Cromer does not disclose or suggest, (or have any apparent reason for) after detection of bootable media for a designated drive, requiring that a user manually input a BIOS boot password in order to boot from the drive.

Thus Cromer clearly does not disclose or suggest all of the features, relationships, and steps recited in the claims. In addition, it would not be obvious to one of ordinary skill in the art at the time of the invention to modify Cromer in a manner that would correspond to the recited subject matter. In paragraph [0010], Cromer holds out as a problem with the prior art, that "it is a trivial exercise for an unauthorized user to connect his own hard disk drive in lieu of the password protected hard disk drive". Cromer's solution to making computers more secure and to prevent any portable unknown drive from being used to boot a computer, is to require the computer to be configured to only boot from devices that internally include data (e.g. model and serial number) that has been previously coupled to the BIOS of the computer. By calling out the disadvantage of

using unknown hard disk drives (e.g. in paragraphs [0010] and [0028]), Cromer teaches away from Applicants' invention (which enables a technician to boot from a new and unknown drive/media) by teaching a system that prevents an unknown device (not coupled to a BIOS) from being booted. Further, since Cromer has provided a method for securely booting from drives (via coupling the drive to the BIOS), there is no apparent reason for one of ordinary skill in the art at the time of the invention to further modify Cromer to require the input of a BIOS boot password, prior to booting from the drive.

In addition, Cromer does not disclose or suggest modifying an automated banking machine to include its described BIOS. An automated banking machine includes ports, such as USB ports inside a locked enclosure and/or a locked safe. Cromer does not provide any teaching or suggestion that such physical security is inadequate.

Further paragraph [0007] of Cromer describes the lack of security associated with an unattended conventional PC. However, automated banking machines are not conventional PCs. For example, even when automated banking machines are unattended, the physical security of ports inside a locked enclosure or chest makes them non-analogous to a vulnerable unattended PC. Thus Cromer does not provide any motivation to one of ordinary skill in the art at the time of the invention to modify an automated banking machine to use his described BIOS.

This recited subject matter does not predictably result from a combination of the applied art, to one of ordinary skill in the art at the time of the invention.

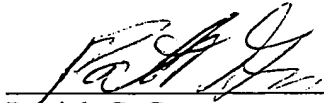
8. In addition, a person of ordinary skill in the art at the time of the invention would consider the applied art as being inoperative and non-enabling with respect to the subject

matter of the claims in the present application. For example, even if there was a generic need in the prior art to make ATMs more secure, such a need could be fulfilled by an unlimited and/or unpredictable number of different features unrelated to the present claims (e.g., hardware dongles, encrypted hard drives, longer passwords, biometric input devices, etc.). With respect to the subject matter of the present claims, a person of ordinary skill in the art could not make or use the claimed invention from the applied art (even if coupled with information known in the art) without undue experimentation. Nowhere does Cromer provide any enabling disclosure which would enable a person of ordinary skill in the art at the time of the invention to hinge a requirement to provide, or not provide a manual input of a BIOS boot password based on the detection of an alternative bootable drive. Such subject matter is not found in Cromer and one of ordinary skill in the art at the time of the invention would not find that such subject matter predictably results from the teachings of Cromer. Cromer does not provide a sufficient enabling disclosure to use or make an automated banking machine have a new BIOS that is configurable with respect to specifying both: that one bootable drive if detected by the BIOS requires a manual input of a BIOS password by a user before booting; and that a second bootable drive does not require manual input by a user of a BIOS password before booting.

9. The applied references do not disclose or suggest and enable all of the features relationships, and steps, recited in the claims. Further, a person of ordinary skill in the art at the time of the invention would not regard the pending claims as being obvious in view of a combination of the applied references based on any of the following rationales:

combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to obtain predictable results; use of known techniques to improve similar devices (methods, or products) in the same way; applying known techniques to a known device (method, or product) ready for improvement to yield predictable results; choosing from a finite number of identified, predictable solutions, each with a reasonable expectation of success; known work in one field of endeavor prompting variations of such known work for use in either the same field or a different field based on design incentives or other market forces in a case where the variations would have been predictable to one of ordinary skill in the art; some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify or to combine prior art reference teachings to arrive at the claimed invention. In conclusion, it was not known nor would it have been obvious to a person having ordinary skill in the art having full view of the cited references, to have produced the claimed features, relationships, and steps.

I hereby declare that all statements herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that the statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both (18 U.S.C. §1001), and may jeopardize the validity of the application or any patent issuing thereon.

  
\_\_\_\_\_  
Patrick C. Green

SEPT 21, 2009  
Date

**Pending Claims in U.S. Application No. 10/620,911 filed July 15, 2003 as set forth in the Amendment responding to the Office Action dated August 12, 2009**

1. A method comprising:

- a) detecting with a computer of an automated banking machine for the presence of a bootable media in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies which of a plurality of storage device drives corresponds to a default storage device drive which does not require an input of a first BIOS password, and which of the plurality of storage device drives corresponds to the at least one alternative storage device drive which does require the input of the BIOS boot password;
- b) booting the computer responsive to a boot record on either the bootable media of the at least one alternative storage device drive or a bootable media of the default storage device drive;

wherein when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password, wherein when the inputted password corresponds to the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot record on the bootable media of the at least one alternative storage device drive; and

wherein when the bootable media of the at least one alternative storage device drive is not detected in step (a), the computer is booted responsive to a boot record on the bootable media of the default storage device drive without requiring a user to input the BIOS boot password.

2. The method according to claim 1, wherein when the bootable media of the at least one alternative storage device drive is detected in step (a) and the BIOS boot password is not inputted within a predetermined amount of time, in step (b) the computer is booted responsive to the boot record of the bootable media of the default storage device drive.
3. The method according to claim 1, wherein when the bootable media of the at least one alternative storage device drive is detected in step (a) and at least once the inputted password does not correspond to the BIOS boot password stored in the BIOS of the computer, in step (b) the computer is booted responsive to the boot record of the bootable media of the default storage device drive.

4. The method according to claim 1, and further comprising:
  - c) executing at least one terminal control software component in the computer which is stored on the bootable media of the default storage device drive; and
  - d) dispensing cash from a cash dispenser responsive to at least one terminal control software component.
5. The method according to claim 1, and further comprising:
  - c) receiving a first input that is representative of a request to run a BIOS setup program; and
  - d) requiring a user to provide a second input that corresponds to the BIOS boot password stored in the BIOS prior to running the BIOS setup program.
6. The method according to claim 1, and further comprising:
  - c) receiving a first input that is representative of a request to run a BIOS setup program; and
  - d) requiring a user to provide a second input that corresponds to a BIOS program password stored in the BIOS prior to running the BIOS setup program.
7. The method according to claim 6, wherein in steps (b) and (c) both the BIOS boot password and the BIOS program password are stored in the BIOS of the computer.
8. The method according to claim 1, wherein in step (b) the default storage device drive and associated bootable media correspond to a hard drive.
9. The method according to claim 8, wherein in step (b) the bootable media of the at least one alternative storage device drive corresponds to a portable media.
10. The method according to claim 9, wherein in step (b) the portable media corresponds to a floppy disk.
11. The method according to claim 9, wherein in step (b) the portable media corresponds to a CD.
12. The method according to claim 9, wherein in step (b) the portable media corresponds to a DVD.
13. The method according to claim 9, wherein in step (b) the portable media corresponds to a portable hard drive.

14. At least one article bearing computer executable instructions operative to cause a computer in an automated banking machine to cause the automated banking machine to carry out a method comprising:

- a) detecting with the computer of the automated banking machine, the presence of a bootable media in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies which of a plurality of storage device drives corresponds to a default storage device drive that does not require an input of a first BIOS password, and which of the plurality of storage device drives corresponds to the at least one alternative storage device drive that does require the input of the BIOS boot password;
- b) booting the computer responsive to a boot record on either the bootable media of the at least one alternative storage device drive or a bootable media of the default storage device drive;

wherein when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password, wherein when the inputted password corresponds to the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot record on the bootable media of the at least one alternative storage device drive; and

wherein when the bootable media of the at least one alternative storage device drive is not detected in step (a), the computer is booted responsive to a boot record on the bootable media of the default storage device drive without requiring a user to input the BIOS boot password.

15. The at least one article according to claim 14, wherein the instructions include a file that is operative to update a flash memory device of the computer of the automated banking machine.

16. A method comprising:

- a) detecting with a computer of an automated banking machine, the presence of a first bootable media in at least one first storage device drive of the automated banking machine;
- b) booting the computer responsive to a boot record on either the first bootable media of the at least one first storage device drive or a second bootable media of a second storage device drive of the automated banking machine;

wherein when the first bootable media is detected in step (a), the booting of the computer includes:



determining responsive to a BIOS of the automated banking machine that the at least one first storage device drive requires a BIOS boot password;

requiring at least once for a user to input the BIOS boot password, wherein when an inputted password corresponds to a BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to a first boot record on the first bootable media; and

wherein when the first bootable media is not detected in step (a) the booting of the computer includes:

determining responsive to a BIOS of the automated banking machine that the second storage device drive does not require the BIOS boot password, wherein the computer is booted responsive to the boot record on the second bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

17. At least one article bearing computer executable instructions operative to cause a computer in an automated banking machine to cause the automated banking machine to carry out a method comprising:

- a) detecting with the computer of the automated banking machine, the presence of a first bootable media in at least one first storage device drive of the automated banking machine;
- b) booting the computer responsive to a boot record on either the first bootable media of the at least one first storage device drive or a second bootable media of a second storage device drive of the automated banking machine;

wherein when the first bootable media is detected in step (a), the booting of the computer includes:

determining responsive to a BIOS of the automated banking machine that the at least one first storage device drive requires a BIOS boot password;

requiring at least once for a user to input the BIOS boot password, wherein when an inputted password corresponds to a BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to a first boot record on the first bootable media; and

wherein when the first bootable media is not detected in step (a) the booting of the computer includes:

determining responsive to a BIOS of the automated banking machine that the second storage device drive does not require the BIOS boot password, wherein the computer is booted responsive to the boot record on the second bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

18. The at least one article according to claim 17, wherein the instructions include a file that is operative to update a flash memory device of the computer of the automated banking machine.

19. A method comprising:

- a) detecting with a computer of an automated banking machine that a bootable media is present in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive;
- b) prompting at least once for a user to input the BIOS boot password;
- c) determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer
- d) booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive;
- e) restarting the computer;
- f) detecting with the computer that a bootable media is not present in the at least one alternative storage device drive; and
- g) booting the computer responsive to a boot record on a bootable media of a default storage device drive without requiring a user to input the BIOS boot password.

20. At least one article bearing computer executable instructions operative to cause a computer in an automated banking machine to cause the automated banking machine to carry out a method comprising:

- a) detecting with the computer of an automated banking machine that a bootable media is present in at least one alternative storage device drive of the automated banking machine, wherein a BIOS of the computer specifies that a BIOS password is required for the bootable media of the at least one alternative storage device drive;

- b) prompting at least once for a user to input the BIOS boot password;
- c) determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer;
- d) booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive;
- e) restarting the computer;
- f) detecting with the computer that a bootable media is not present in the at least one alternative storage device drive; and
- g) booting the computer responsive to a boot record on a bootable media of a default storage device drive without requiring a user to input the BIOS boot password.

21. The at least one article according to claim 20, wherein the instructions include a file that is operative to update a flash memory device of the computer of the automated banking machine.

22. An automated banking machine comprising:

a computer, wherein the computer includes a BIOS, wherein the BIOS includes a BIOS boot password, and wherein the BIOS specifies a default storage device drive which does not require a boot password;

at least one input device in operative connection with the computer;

at least one transaction function device in operative connection with the computer; and

at least one first storage device drive and a second storage device drive in operative connection with the computer, wherein the second storage device drive corresponds to the default storage device drive specified in the BIOS, wherein when the computer detects a bootable media associated with the at least one first storage device drive, the computer is operative to require a user to input a BIOS boot password through the at least one input device prior to booting responsive to a boot record associated with the bootable media of the at least one first storage device drive, wherein when the computer does not detect a bootable media associated with the at least one first storage device drive, the computer is operative to boot responsive to a boot record on a bootable media of the second storage device drive without requiring a user to input the BIOS boot password.

23. The machine according to claim 22, wherein when the bootable media of the at least one first storage device drive is detected by the computer and the BIOS boot password has not been inputted thorough the at least one input device within a predetermined amount of time, the computer is operative to automatically boot responsive to the boot record associated with the bootable media of the second storage device drive.

24. The machine according to claim 22, wherein when the bootable media of the at least one first storage device drive is detected by the computer and at least one password inputted through the at least one input device does not correspond to the BIOS boot password, the computer is operative to automatically boot responsive to the boot record associated with the bootable media of the second storage device drive.

25. The machine according to claim 22, wherein the second storage device drive and associated bootable media corresponds to a hard drive.

26. The machine according to claim 25, wherein the bootable media for the at least one first storage device drive includes a portable bootable media.

27. The machine according to claim 26, wherein the portable bootable media includes a floppy disk.

28. The machine according to claim 26, wherein the portable bootable media includes a CD.

29. The machine according to claim 26, wherein the portable bootable media includes a DVD.

30. The machine according to claim 26, wherein the portable bootable media includes a portable hard drive.

31. The machine according to claim 22, wherein the at least one first storage device drive corresponds to a first portable storage device drive and a second portable storage device drive, wherein the second storage device drive corresponds to a hard drive, wherein the BIOS includes a boot order, wherein the boot order specifies a sequence for storage device drives in which the computer is operative to attempt to boot from, wherein the boot order includes the sequence of: the first portable storage media device drive, the second portable storage media device drive and the hard drive.

32. The machine according to claim 22, wherein the computer includes a BIOS setup program, wherein the computer is operative to require that a user input through the at least one input device, the BIOS boot password prior to being granted access to modify the BIOS through the BIOS setup program.

33. The machine according to claim 22, wherein the computer includes a BIOS setup program and a BIOS program password, wherein the computer is operative to require that a user input through the at least one input device, the BIOS program password prior being granted access to modify the BIOS with the BIOS setup program.

34. The machine according to claim 22, wherein the transaction function device includes a cash dispenser, wherein when the computer has booted responsive to the boot record of the bootable media of the second storage device drive, the computer is operative to cause the cash dispenser to dispense cash responsive to at least one further input through the at least one input device.

**(x)**

**RELATED PROCEEDINGS APPENDIX**

None.